United States Government Accountability Office

GAO

Report to Congressional Requesters

August 2007

DEFENSE INFRASTRUCTURE

Management Actions Needed to Ensure Effectiveness of DOD's Risk Management Approach for the Defense Industrial Base

GAO-07-1077

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Infrastructure. Management Actions Needed to Ensure Effectiveness of DOD's Risk Management Approach for the Defense Industrial Base	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **General Accountability Office,441 G Street NW,Washington,DC,20548**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**42**	

August 2007

DEFENSE INFRASTRUCTURE

Management Actions Needed to Ensure Effectiveness of DOD's Risk Management Approach for the Defense Industrial Base

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-1077, a report to congressional requesters

Why GAO Did This Study

The U.S. military relies on the defense industrial base (DIB) to meet requirements to fulfill the National Military Strategy. The potential destruction, incapacitation, or exploitation of critical DIB assets by attack, crime, technological failure, natural disaster, or man-made catastrophe could jeopardize the success of U.S. military operations. GAO was asked to review the Department of Defense's (DOD) Defense Critical Infrastructure Program and has already reported that DOD has not developed a comprehensive management plan for its implementation. This, the second GAO report, has (1) determined the status of DOD's efforts to develop and implement a risk management approach to ensure the availability of DIB assets, and (2) identified challenges DOD faces in its approach to risk management. GAO analyzed plans, guidance, and other documents on identifying, prioritizing, and assessing critical domestic and foreign DIB assets and held discussions with DOD and contractor officials.

What GAO Recommends

GAO recommends that DOD take specific actions to implement its risk management framework. DOD partially concurred with all of GAO's recommendations. DOD's comments cited actions it planned to take that are generally responsive to our recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-1077.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Davi M. D'Agostino, (202) 512-5431 or dagostino@gao.gov.

What GAO Found

DOD has begun developing and implementing a risk management approach to ensure the availability of DIB assets needed to support mission-essential tasks, though implementation is still at an early stage. Its sector assurance and sector-specific plans focus on steps to identify a list of critical assets that, if damaged, would result in unacceptable consequences; prioritize those critical assets based on a risk assessment process; perform vulnerability assessments on high-priority critical assets, and encourage contractors' actions to remediate or mitigate adverse effects found during these assessments, as appropriate, to ensure continuity of business. The Defense Contract Management Agency, the executing agency for the DIB, has developed a process to identify the most important DIB assets and to narrow this list to those it considers critical. It has also developed an asset prioritization model for determining a criticality score and ranking critical assets, and it has established a standardized mission assurance vulnerability assessment process for critical DIB assets.

DOD faces several key challenges in implementing its DIB risk management approach. Overall, DOD's methodology for identifying critical DIB assets is evolving, and DOD lacks targets and time frames for completing development of key program elements that are needed for its risk management approach. Without them, DOD cannot measure its progress toward ensuring that DIB assets supporting critical DOD missions are properly identified and prioritized. The specific challenges are as follows: First, DOD is not fully incorporating the military services' mission-essential task information (i.e., listings of assets whose damage, degradation, or destruction would result in DOD-wide mission failure) in compiling its critical asset list. Second, GAO's analysis of DOD's prioritization model shows that weighting factors were selected and data determined according to subjective decisions and limited review, and that needed contractor-specific data were lacking, as was comprehensive threat information, thus undermining the utility of the index score for prioritizing contractors. Without these comprehensive data and a reliable asset prioritization model, DOD will not be in a sound position to know that it has identified the most important and critical assets, as called for in the National Military Strategy. Third, with regard to scheduling and conducting assessments of critical DIB assets, DOD is currently doing so based on contractor amenability and security clearance status without regard for assets' priority rankings, and thus cannot ensure that the most critical DIB contractors are assessed. Fourth, DOD lacks a plan for developing options to work with the Department of State and other appropriate agencies to identify and address potential challenges in assessing vulnerabilities in foreign critical DIB assets. Until all these challenges are addressed, DOD will lack the visibility it needs over critical DIB asset vulnerabilities, will be unable to encourage critical DIB contractors to take needed remediation actions, and will be unable to make informed decisions regarding limited resources.

Contents

Abbreviations

ASD-HD	Assistant Secretary of Defense for Homeland Defense
ASD(HD&ASA)	Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
CBRNE	Chemical/biological/radiological/nuclear/explosive
CIP-MAA	Critical Infrastructure Program—Mission Assurance Assessment
DCIP	Defense Critical Infrastructure Program
DCMA	Defense Contract Management Agency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	Defense Industrial Base
DOD	Department of Defense
DSS	Defense Security Service
DTRA	Defense Threat Reduction Agency
FBI	Federal Bureau of Investigation
HSPD-7	Homeland Security Presidential Directive 7
MSA	Metropolitan Statistical Area
OSD	Office of the Secretary of Defense
PCII	Protected Critical Infrastructure Information
USD(AT&L)	Undersecretary of Defense for Acquisition, Technology, and Logistics
USD(P)	Under Secretary of Defense for Policy

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

August 31, 2007

The Honorable Solomon P. Ortiz
Chairman
The Honorable Jo Ann Davis
Ranking Member
Subcommittee on Readiness
Committee on Armed Services
House of Representatives

The Honorable W. Todd Akin
House of Representatives

The U.S. military relies on the defense industrial base (DIB) to meet military requirements to fulfill the National Military Strategy. The DIB is the government and private-sector worldwide industrial complex with capabilities to perform research and development and design, produce, and maintain military weapons systems, subsystems, components, and parts. The DIB comprises hundreds of thousands of industrial sites, and the preponderance of the DIB is privately owned and includes businesses of all sizes. The potential destruction, incapacitation, or exploitation of critical DIB assets by terrorist attack, criminal activity, technological failure, natural disaster, or man-made catastrophe could jeopardize the success of U.S. military operations. For example, reliance on a single source contractor having the unique capability to make an industrial part or material critical to a mission could significantly affect warfighter operations if that material were not available because of a flood at the site of the manufacturing facility.

Homeland Security Presidential Directive 7 (HSPD-7),[1] issued in December 2003, designates the Secretary of the Department of Homeland Security (DHS) as the principal federal official to lead, integrate, and coordinate the implementation of efforts among the federal departments and agencies, state and local governments, and the private sector to protect the nation's critical infrastructure and key resources.

[1]*Homeland Security Presidential Directive 7* (Washington D.C., Dec. 17, 2003).

In addition, the Homeland Security Act of 2002 and HSPD-7 directed DHS to produce a national plan for critical infrastructure and key resources protection. DHS issued the National Infrastructure Protection Plan on June 30, 2006. This plan provides the framework for developing, implementing, and maintaining a coordinated national effort. The plan also identifies 17 infrastructure and key asset sectors, and it designates one or more lead federal agencies—referred to as "sector-specific agencies"—for each sector. For example, DHS is the sector-specific agency for 10 of the 17 sectors, including information technology, transportation, and chemicals; the Department of Health and Human Services is the sector-specific agency for public health and healthcare; and the Department of Defense (DOD) is the sector-specific agency for the DIB. Sector-specific agencies are responsible for, among other things, collaborating with all relevant federal, state, and local governments and the private sector; encouraging risk management strategies; and conducting or facilitating vulnerability assessments of their sector.

The cornerstone of the National Infrastructure Protection Plan is its risk-management framework, which establishes priorities based on risk and calls for protection and business continuity initiatives that provide the greatest mitigation of risk. The National Infrastructure Protection Plan also requires each of the sector-specific lead agencies to submit a plan outlining its approach, following guidance established by DHS, by December 2006.

Within DOD, the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD[HD&ASA]), serves as the principal civilian advisor to the Secretary of Defense on the identification, prioritization, and protection of DOD's defense critical infrastructure.[2] DOD Directive 3020.40, issued in August 2005, updates DOD policy and assigns responsibilities for DOD's Defense Critical Infrastructure Program (DCIP), incorporating guidance from HSPD-7. This directive assigns defense sector lead agents for 10 sectors within the DCIP, 1 of which is the DIB.[3] For DOD's efforts relating to the DIB as critical

[2]The Office of the Under Secretary of Defense for Policy was reorganized in December 2006. This reorganization included, among other things, the Office of the Assistant Secretary of Defense for Homeland Defense being renamed the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs. Hereafter, this office is referred to by its current name.

[3]The 10 defense sectors are defense industrial base; financial services; global information grid; intelligence, surveillance, and reconnaissance; space; health affairs; logistics; personnel; public works; and transportation.

infrastructure, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]), in coordination with the Under Secretary of Defense for Policy (USD[P]), integrates DCIP policies with acquisition, technology, and logistics policy guidance; identifies vulnerabilities in technologies relied upon by DOD critical infrastructure and develops countermeasures; and provides coordination, guidance, and monitoring. The Defense Contract Management Agency (DCMA) is designated the sector lead agent for the DIB.

Recognizing that it is not feasible to protect its entire infrastructure against every possible threat, the umbrella DCIP pursues a risk-management approach to prioritize resources and operational requirements in its DIB efforts. As we have previously reported,[4] risk management is a systematic, analytical process to consider the likelihood that a threat will harm critical assets and then to identify actions to reduce the risk and mitigate the potential consequences of the threat. While risk generally cannot be eliminated, it can be reduced by taking actions such as establishing backup systems to protect against or reduce the effect of an incident. DOD's risk management approach is based on assessments of threats, vulnerabilities, and criticality, and requires DCMA to identify and prioritize its most critical assets, assess vulnerabilities, and identify remediation requirements. At the same time, DOD is identifying its mission-essential tasks. It expects this identification to help clarify the criticality of key assets for accomplishing its missions.

You asked that we review a number of issues related to DOD's DCIP. To address them, we committed to issuing two reports in response to your request. Our first report, issued in May 2007, examined the extent to which DOD has developed a comprehensive management plan and the actions needed to guide its efforts to identify, prioritize, and assess non-DIB sectors in its critical infrastructure under DCIP. [5] We found that DOD had taken some important steps to implement DCIP, but it had not developed a comprehensive management plan containing key elements, including the development and issuance of guidance, the coordination of stakeholders' efforts, and the identification of resource requirements and sources to

[4]GAO, *Homeland Security: Key Elements of a Risk Management Approach*, GAO-02-150T (Washington, D.C.: Oct. 12, 2001); *Defense Infrastructure: Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure*, GAO-07-461 (Washington, D.C.: May 24, 2007).

[5]GAO-07-461.

guide its efforts.[6] We recommended that DOD develop and implement such a plan and, among other things, assist the defense sector lead agents in identifying, prioritizing, and funding the DCIP, including developing funding requirements through the regular budgeting process. DOD concurred with all of our recommendations.

For this second report, we (1) determined the status of DOD's efforts to develop and implement a risk management approach to ensure the availability of DIB assets to support mission-essential tasks; and (2) identified challenges DOD faces in its approach to risk management in the DIB sector.

To examine the status of DOD's efforts to develop and implement a risk management approach, we reviewed the DIB sector-specific and sector assurance plans and other studies; and discussed with DOD officials the requirements for a risk management plan for the DIB and the status of DOD's implementation of the approach. We also reviewed and discussed information on DCMA's efforts to identify, assess, and remediate critical DIB assets; the criteria DCMA established and used to identify important DIB assets and critical DIB assets; the asset prioritization model and the factors used to rank order the critical assets; the standardized mission assurance assessment process for critical DIB assets; and the remediation planning guidance for the DCIP generally, including the guidance being developed for the DIB. We also examined standards developed for vulnerability assessments to be done at contractor facilities and met with the National Guard Bureau and one of the state National Guard teams that conducts DIB sector vulnerability assessments.

To examine the challenges faced by DOD in developing and implementing its approach, we compared the policies for identifying mission-essential tasks and related defense critical assets with DCMA's approach to identifying a critical DIB asset list; and examined the development and use of DCMA's asset prioritization model, including requirements for models to undergo external technical review and methods used to obtain contractor-specific data as needed input into the model. We reviewed and discussed with each of the services their DCIP efforts related to the DIB,

[6]See, for example, GAO, *Military Readiness: Navy's Fleet Response Plan Would Benefit from* a *Comprehensive Management Approach and Rigorous Testing*, GAO-06-84 (Washington, D.C.: Nov. 22, 2005); as well as GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999), which emphasizes the importance of such a plan to guide program implementation.

including their responses to DCMA regarding its requests for the services to update the important and critical DIB asset lists. Also, we discussed with several DOD intelligence agency officials the threats to the DIB and the availability of specific threat information to DCMA. We discussed with DCMA officials the challenges that they have encountered as they have begun working with private sector contractors; and efforts to encourage private-sector DIB contractors to participate in the program. We also spoke with a non-probability sample of DIB contractor officials and asked them generally about their willingness to participate in the program. We discussed with DOD officials and these contractor officials the availability of data on foreign contractors. Their comments are not generalizable to a larger population. Lastly, we determined the extent to which DCMA has identified metrics with time frames for completing development of the risk-based management process. A more thorough description of our scope and methodology is provided in appendix I. We conducted our work between August 2006 and June 2007 in accordance with generally accepted government auditing standards.

Results in Brief

DOD has developed and begun implementing a risk management approach, as called for in the National Infrastructure Protection Plan, to ensure the availability of critical DIB assets needed to support mission essential tasks, though implementation is still in an early stage. The approach comprises two plans. First, the DIB sector assurance plan, issued in May 2005 and updated in May 2007, outlines an approach for identifying vulnerabilities, risks, and effect on business; implementing remediation and mitigation strategies; and managing consequences to ensure continuity of operations. Second, the DIB sector-specific plan, submitted in December 2006, outlines DOD's approach to executing its sector-specific responsibilities, follows guidance established by DHS, and complements other DOD critical infrastructure policy. It focuses efforts on assets, systems, networks, and functions that, if damaged, would result in unacceptable consequences to the DOD mission, national economic security, public health and safety, or public confidence. The sector assurance plan provides a coordinated strategy for managing risk at DIB critical asset sites located throughout the world and describes a risk management approach and plans for the DIB. It focuses on steps to (1) identify a critical asset list; (2) prioritize the critical assets on that list; (3) perform vulnerability assessments on high-priority critical assets; and (4) encourage contractors' actions to remediate or mitigate adverse effects found during these assessments, as appropriate, to ensure continuity of business operations. In implementing the sector assurance plan, DCMA has taken actions in each of these four areas. It has developed a process to

identify the most important DIB assets and to narrow this list to those it considers critical using a tiered approach that enables identification of important capabilities and critical assets from the hundreds of thousands of entities constituting the DIB. It has developed an asset prioritization model for determining a criticality score and ranking critical assets, thus providing a mechanism for allocating the resources available to those critical assets assessed to be most vulnerable. It has established a standardized mission assurance vulnerability assessment process for critical DIB assets and, as of June 1, 2007, had completed eight assessments for which reports had been issued. Lessons learned from these assessments have been incorporated into training for the assessments scheduled for fiscal year 2007. Concurrently, ASD(HD&ASA) has been developing a remediation planning guide for the DCIP. The planning guide calls for an effective plan of action and milestones focusing on a remediation strategy to be developed as soon as feasible following the risk assessment. The planning guide includes a chapter focused on DIB remediation, but states that the remediation measures for the DIB focus on facilitating relationships and sharing information to implement the appropriate level of protection and does not suggest any time frames because of the voluntary nature of the DIB participation in the DCIP.

DOD faces several key challenges in implementing its DIB risk management approach and will need to address them to ensure that its approach is sound and its progress can be measured. First, DCMA is not currently obtaining comprehensive information from all of the combatant commands and services needed to develop a critical asset list that is linked to DOD's mission-essential tasks. Second, DCMA's prioritization model has not yet undergone external technical review, lacks needed contractor-specific data, and lacks comprehensive threat information. Third, DCMA is conducting its vulnerability assessments of contractors without regard for their prioritization rankings. Fourth, DOD lacks a plan for identifying and addressing challenges in assessing vulnerabilities in foreign DIB critical assets. More specifically:

- Both the 2006 DIB critical asset list and the list in development for 2007 do not reflect data from all the combatant commands and services using mission-essential task information. The DOD risk management approach calls for identifying DIB assets critical to supporting combatant commanders' mission-essential tasks that would result in DOD-wide mission failure if the asset were to be damaged, degraded, or destroyed. DOD has not established a plan with targets and time frames for identifying all of the mission-essential tasks for all of the services.

- Our analysis of the model revealed that weighting factors were selected and much of the input data were determined according to subjective decisions made with only limited review. Furthermore, the model does not distinguish between contractors who are marked as high risk by default for lack of data, and those for whom data exist and corroborate that designation. DOD collects open-source and in-house statistical data on contractor operations, but it lacks some needed contractor-specific information from the DIB contractors on their operations for use in the model. DCMA has undertaken two surveys to obtain these needed data and is planning a third survey. However, these collection efforts did not receive high response rates, and they yielded problematic data quality. Currently, DCMA lacks a detailed plan for improving response rates and data quality in its next survey. In addition, DCMA does not yet receive or have procedures to obtain comprehensive threat information from appropriate intelligence agencies, including DHS, the Federal Bureau of Investigation (FBI), and others, needed to enable it to accurately prioritize DIB assets. The absence of threat information from the appropriate intelligence agencies undermines the utility of the index score for prioritizing contractors.
- DCMA is conducting its vulnerability assessments on critical DIB assets according to contractor accessibility and security clearance status, without regard for those assets' respective prioritization model rankings. The DOD risk management approach calls for DCMA to schedule and conduct its vulnerability assessments on the critical DIB assets based upon their respective rankings as validated in the asset prioritization model.
- DCMA has not yet established a plan to address the potential challenges inherent in obtaining data from and assessing vulnerabilities of critical foreign contractors. In order to do so, DCMA needs to coordinate with other agencies, such as the Department of State, to develop strategies to better ensure that foreign contractor vulnerabilities can be identified and addressed. DCMA has not conducted any vulnerability assessments of foreign contractors, but has begun to take steps in examining this issue.

This report makes recommendations that DOD take specific actions to implement its risk management framework by: (1) developing a comprehensive DIB critical asset list that includes the services' mission-essential task information as well as data based on current DCMA criteria; (2) ensuring that its asset prioritization model is reliable by obtaining external technical review, needed contractor-specific data, and comprehensive threat information; (3) conducting vulnerability assessments of critical contractors based on their rankings according to the asset prioritization model; and (4) preparing a plan to collaborate with appropriate agencies to develop options to better ensure that foreign

contractor vulnerabilities can be identified and addressed. In written comments on the draft report, DOD partially concurred with all of our recommendations. In its response, DOD cited actions it planned to take that are generally responsive to our recommendations. DOD also provided us with technical comments, which we incorporated in the report, as appropriate. DOD's response is reprinted in appendix II.

Background

According to DOD's Strategy for Homeland Defense and Civil Support, dated June 2005, without the important contributions of the private sector, DOD cannot effectively execute its core defense missions. Private industry manufacturers provide the majority of equipment, materials, services, and weapons for the U.S. armed forces. The President designated DOD as the sector-specific agency for the DIB. In this role, DOD is responsible for collaborating with all relevant federal departments and agencies, state and local governments, and the private sector; encouraging risk management strategies; and conducting or facilitating vulnerability assessments of the DIB as set forth in HSPD-7.

In executing these responsibilities, the Secretary of Defense requires a network of organizations with diverse roles and missions. Key participants in the network include the following:

- The Undersecretary of Defense for Acquisition, Technology, and Logistics, USD(AT&L), who is responsible for, among other things, integrating DCIP policies into acquisition, procurement, and installation policy guidance and for coordinating with ASD(HD&ASA) to ensure DCIP-related guidance is developed and implemented, and that system providers remediate vulnerabilities identified prior to system fielding or deployment.
- ASD(HD&ASA), which serves as the principal civilian advisor to the Secretary of Defense on the identification, prioritization, and protection of DOD's critical infrastructure. ASD(HD&ASA) assigned responsibility for the DCIP, including DIB sector-specific agency responsibilities, to the Director for Critical Infrastructure Protection under the Deputy Assistant Secretary of Defense for Crisis Management and Defense Support to Civil Authorities. The DCIP office provides policy, program oversight, integration, and coordination of activities.
- DCMA, which is the defense sector lead agent responsible for the coordination and oversight of DCIP matters pertaining to the DIB because of DCMA's established working relationship with DIB owners/operators. DCMA responsibilities include planning and coordinating with all DOD components and private-sector partners that own or operate elements of the DIB.

- Private-sector owners, operators, and organizations; and other federal departments and agencies, including DHS, the FBI, and the Departments of Energy, Commerce, the Treasury, and State. It also includes state and local agencies, international organizations, and foreign countries.

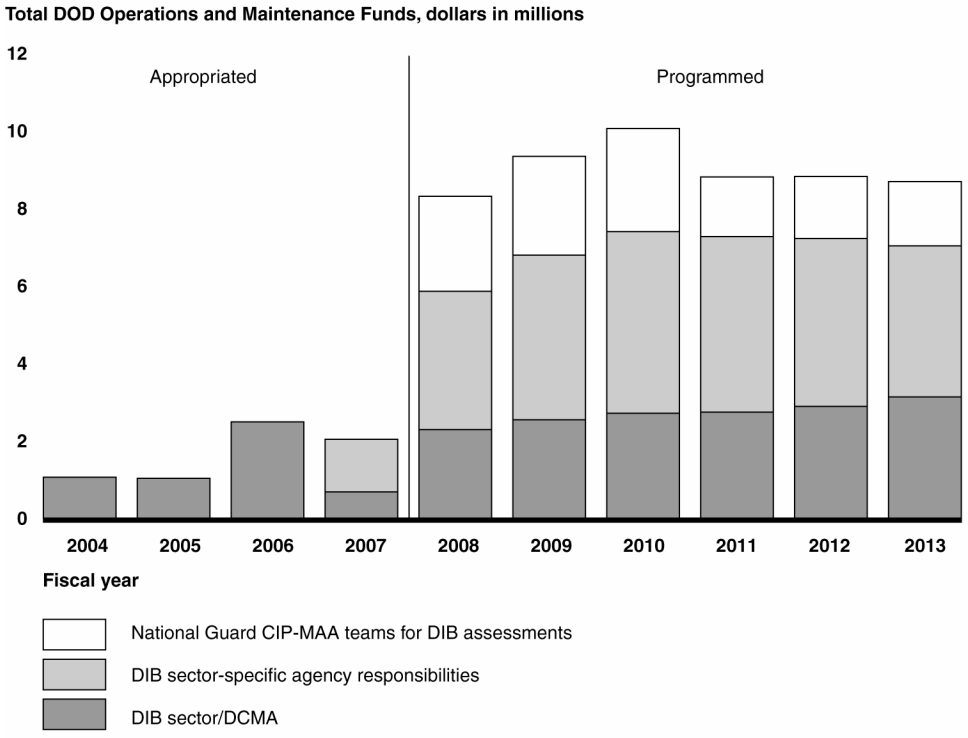
Under Homeland Security Presidential Directive 7, federal departments and agencies are to identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit the infrastructure and resources; and they are to work with state and local governments and the private sector to accomplish this objective. Sector-specific agencies, among other things, are to encourage risk management strategies to protect against and mitigate the effect of attacks against critical infrastructure and key resources.

DOD's risk management approach is based on assessing threats, vulnerabilities, criticalities, and the ability to respond to incidents. Threat assessments identify and evaluate potential threats on the basis of capabilities, intentions, and past activities. Vulnerability assessments identify potential weaknesses that may be exploited and recommend options to address those weaknesses. Criticality assessments evaluate and prioritize contractors on the basis of their importance to mission success. These assessments help prioritize limited resources and thus, if implemented properly, would reduce the expense of resources on lower-priority contractors. DOD's risk management approach also includes an assessment of the ability to respond to, and recover from, an incident.

ASD(HD&ASA) officials said it provided research and development funding for program development in fiscal years 2005 and 2006 of $550,000 and $675,000, respectively. It did not provide research and development funding to DCMA in 2007 and said it did not intend to provide any during the period of fiscal years 2008 to 2013. They said that for operations and maintenance, DOD funded the program at about $1.1 million and $1.0 million in fiscal years 2004 and 2005, respectively; and $2.5 million and $2.0 million in fiscal years 2006 and 2007, respectively. DOD plans to increase operations and maintenance funding to about $8.3 million in fiscal year 2008, about $9.4 million in 2009, and about $10.1 million in 2010 before decreasing it to about $8.8–$8.7 million in subsequent fiscal years through fiscal year 2013. In January 2007, the Joint Requirements Oversight Council, chaired by the Vice Chairman of the Joint Chiefs of Staff, approved the National Guard Critical Infrastructure Program—Mission Assurance Assessment (CIP-MAA) capability for the DIB. The council agreed that the services will provide funding to meet the

requirements for fiscal years 2008–2013, and it endorsed the National Guard as the overall lead agency to implement the CIP-MAA. The operations and maintenance funding is summarized in figure 1.

Figure 1: Operations and Maintenance Funding for DIB Activities for Fiscal Years 2004 to 2007 and Programmed Funding for Fiscal Years 2008 to 2013



Source: ASD(HD&ASA).

DOD Has Begun Developing and Implementing a Risk Management Approach to Ensure the Availability of the DIB

DOD has begun developing and implementing a risk management approach to ensure the availability of DIB assets needed to support mission-essential tasks, though implementation is still at an early stage. The approach comprises two plans. First, the DIB sector assurance plan, issued in May 2005 and updated in May 2007, outlines an approach for identifying vulnerabilities, risks, and effect on business; implementing remediation and mitigation strategies; and managing consequences to ensure continuity of operations.[7] Second, the DIB sector-specific plan, submitted in December 2006, outlines DOD's approach to executing its sector-specific responsibilities, follows guidance established by DHS, and complements other DOD critical infrastructure policy.[8] It focuses efforts on assets, systems, networks, and functions that, if damaged, would result in unacceptable consequences to the DOD mission, national economic security, public health and safety, or public confidence. The sector assurance plan provides a coordinated strategy for managing risk at DIB critical asset sites located throughout the world and describes a risk management approach and plans for the DIB. It focuses on steps to (1) identify a critical asset list; (2) prioritize the critical assets on that list; (3) perform vulnerability assessments on high-priority critical assets; and (4) encourage contractors' actions to remediate or mitigate adverse effects found during these assessments, as appropriate, to ensure continuity of business operations.

DOD depends on the DIB to accomplish its work in support of military missions. The absence or unavailability of some assets designated as critical DIB assets, and the products and services these assets produce, could cause military mission failure. To identify DIB critical assets, DCMA industrial analysts and other DOD personnel compiled a list of approximately 900 important defense contractor assets, and then narrowed this number by using another set of criteria. DCMA has also developed an asset prioritization model for determining a criticality score and ranking critical assets, from highest to lowest risk. It has established a standardized mission assurance vulnerability assessment process for critical DIB assets, and as of June 1, 2007, had completed and issued

[7]DOD, Assistant Secretary of Defense for Homeland Defense (ASD [HD&ASA]), *Defense Industrial Base (DIB) Defense Infrastructure Sector Assurance Plan (DISAP)* (Washington, D.C., May 2, 2005); DOD, *Defense Industrial Base Defense Sector Assurance Plan* (Washington, D.C., May 14, 2007).

[8]DOD, *Sector Specific Plan for the Defense Industrial Base* (Washington, D.C., Dec. 27, 2006).

reports for eight assessments and had three other assessments in process. ASD(HD&ASA) is developing guidance to provide a standardized process for determining, planning, and implementing remediation actions for DOD personnel involved in remediating risks and supporting overall DOD mission assurance. Table 1 provides a summary of the current number of important and critical DIB assets identified and the number of contractors assessed.

Table 1: A Summary of DOD's Efforts in Identifying and Assessing Critical DIB Assets as of June 1, 2007

		Critical contractors		
DIB assets	**Important contractors**	**Domestic**	**Foreign**	**Total**
Identified	900	194	9	**203**
Assessed[a]		8	0	**8**

Source: GAO analysis of DCMA data.

[a]The number of contractors assessed does not include 5 that were completed prior to DCMA's pilot program being established.

DCMA Has Taken Steps to Identify Critical Assets

DCMA has developed a process to identify the most important DIB assets and to narrow this list to those it considers critical using a tiered approach that enables identification of important capabilities and critical assets from the hundreds of thousands of entities constituting the DIB. The collection of data on each entity within the DIB was considered neither practical nor an effective use of limited resources, so DCMA focused on reducing the magnitude of assets to a manageable number through the use of government DIB subject-matter experts. DCMA has developed a process to identify the most important DIB assets and to narrow this list to those it considers critical. The criteria used for both lists are shown below in table 2.

Table 2: DCMA Criteria Used to Identify Important and Critical DIB Assets

"Important" if they satisfy one or more of the following criteria:	"Critical" if they satisfy one or more of the following criteria:
• They are a sole source. • They use obsolete/enabling/emerging technology. • They require a long lead time. • They lack surge production. • They have a significant cost escalation.	• They are a prime or subcontractor single source with unique technology or industrial capability that could significantly affect warfighter operations due to nonavailability of material. • They are a prime contractor with capabilities that support numerous programs or industries. • They are a single source subcontractor with a long requalification time that supports numerous programs across the services. • They are an essential advanced technology source.

Source: DCMA.

The critical asset list is reviewed, updated, and approved annually. DCMA identifies potential assets meeting the criteria, and the military services and defense agencies then validate and update the list. DCMA reviews and validates the updated list and prioritizes it using the asset priority model. DCMA then coordinates with senior acquisition executives and submits the revised critical asset list for approval to the Deputy Under Secretary of Defense for Industrial Policy, USD(AT&L), and ASD(HD&ASA).

DCMA Has Been Developing an Asset Prioritization Model

DCMA has been developing an asset prioritization model for determining a criticality score and ranking critical assets from highest to lowest risk. This model is to provide a mechanism for DCMA to allocate limited resources to those critical DIB assets assessed to be most vulnerable: the higher the score, the higher the priority of the asset for vulnerability assessment and possible remediation/mitigation actions. The model uses 16 weighted factors that are aggregated to assign a vulnerability score to each asset. These factors are broadly classified into mission (5), economic (4), threat (5), and other (2), as shown below in table 3.

Table 3: DCMA's Asset Prioritization Model Factors, Weighting Factors, and Factor Classification

Model factors	Weighting factors	Factor classification
Affect multiple programs	16	Mission
Affect current warfighting capabilities	15	Mission
Effect on projected warfighting capabilities	14	Mission
Corporate financial risk	13	Economic
Site economic viability	12	Economic

Model factors	Weighting factors	Factor classification
Recovery plan	11	Mission
Reconstitution—time	10	Mission
Reconstitution—cost	9	Economic
Threat—known external threats to facility	8	Threat
Known security issues	7	Threat
Disaster risk—metric	6	Threat
Chemical/biological/radiological/nuclear/explosive (CBRNE) collateral damage	5	Threat
Populated area	4	Threat
Site employment as percent of county or Metropolitan Statistical Area (MSA)	3	Economic
DCIP awareness visit follow-up	2	Other
Vulnerability assessment of CIP-MAA completed/scheduled	1	Other

Source: DCMA.

Data for the determination of these factors are collected from DCMA surveys and analysis, supplemented by various commercial and government sources, including the Defense Logistics Agency, the military services, and the combatant commands. If there are missing data for a given item, DCMA's rule is to default to a high-risk score, as this is the most conservative assumption.

For threat data currently obtained by DCMA, the model includes an assessment of current, potential, and technologically feasible threats to assets from hostile parties as well as from natural or accidental disasters inherent to the asset or its location. Hostile threat information is collected by the Counter Intelligence Field Activity office from various intelligence sources and then summarized in a threat assessment document for specific sites during the prioritization process, and in a detailed threat assessment prior to conducting an actual National Guard assessment of a site. The Counter Intelligence Field Activity has also established an arrayed threats data system as the DIB sector's primary method for obtaining threat-related information.

DCMA Has Established a Standardized Vulnerability Assessment Process

DCMA has established a standardized mission assurance vulnerability assessment process for critical DIB assets. As of June 1, 2007, it had completed and issued eight assessment reports. Lessons learned from

earlier assessments have been incorporated into training for the assessments scheduled for fiscal year 2007.

The current approach for performing assessments has evolved from earlier efforts designed to protect the mission of the asset from a broad spectrum of threats. The approach calls for multidisciplinary teams to conduct performance-based assessments to identify vulnerabilities of critical missions and recommend ways to mitigate those vulnerabilities. DOD found these efforts to be effective, but costly and time consuming. It developed a set of standards to conduct vulnerability assessments, building on other vulnerability assessment methods DOD has used. Working through DCMA and the National Guard Bureau, DOD has established a standardized mission assurance assessment for application to critical DIB assets. These assessments consider effect, vulnerability, and threat/hazard from natural disaster, technological failure, human error, criminal activity, or terrorist attack. To perform assessments, DCMA partners with the Defense Security Service (DSS), the Counter Intelligence Field Activity, the Defense Intelligence Agency (DIA), and appropriate federal, state, and local law enforcement to identify and characterize all hazard threats to key assets, and uses benchmarks and standards to ensure consistency within the DIB and the broader DCIP community.

The assessment process typically involves (1) using the critical asset list to select the DIB contractor candidate for assessment; (2) notifying the selected DIB asset to schedule the vulnerability assessment; (3) conducting a preassessment briefing with the contractor; (4) scheduling the assessment; (5) negotiating a memorandum of agreement with the contractor to coordinate the terms of the assessment; (6) performing the assessment, which is designed to assess vulnerability to a broad spectrum of threats; (7) providing an outbriefing; and (8) writing a final vulnerability assessment report.

The process for conducting vulnerability assessments on critical DIB contractors is early in implementation and only 8 of the planned 203 have been completed, with reports issued, as of June 1, 2007. DCMA estimated that conducting assessments on all critical DIB assets will take several years. Between fiscal years 2003 and 2006, DOD considered and evaluated different approaches that might be used in conducting on-site vulnerability assessments. For example, five assessments of different types were done by different DOD groups prior to fiscal year 2006. With the benefit of the earlier assessments, DCMA in fiscal year 2006 developed a pilot project that included six vulnerability assessments and used the information gained to develop an approach for conducting on-site vulnerability

assessments at all critical DIB asset locations. DCMA had settled on a methodology for outreach to contractors, a standardized approach for conducting on-site vulnerability assessments,[9] and training for National Guard teams to conduct these assessments. DCMA is planning a number of improvements as a result of lessons learned from the six pilot project assessments. For example, DCMA officials said they planned to update the existing benchmarks, develop additional benchmarks for security operations and emergency management, and determine the final report format to use for future assessments. In addition, DCMA officials said that, as a result of the pilot assessments, they plan to change the process on future assessments. For example, rather than a single visit to the contractor to perform the entire assessment, they intend to conduct an advance site visit to identify key officials, gather information, and perform preliminary analyses on manufacturing and infrastructure. They said this will allow more time for up-front analysis and alleviate the workload and reduce the hours needed at the time of the assessment visit.

In fiscal year 2007, DCMA planned to have National Guard teams conduct 19 vulnerability assessments and then to increase its pace to complete these vulnerability assessments at a rate of 50 per year. However, it has changed this goal for 2007, and even at the rates planned it would take 6 years, or until 2012, to complete the initial vulnerability assessments on the 203 critical DIB contractors identified in 2006, as shown in table 4.

Table 4: Assessments Planned during Fiscal Years 2007 to 2012

Fiscal year	2007	2008	2009	2010	2011	2012
Assessments planned as of November 2006	19	50	50	50	20	20
Revised plan as of May 2007[a]	14	21	21	50	50	50

Source: DCMA.

[a]DCMA is planning that after completing the initial assessments, DIB assets would be reassessed every 3 years.

[9]This approach uses benchmarks involving a series of questions determining the degree to which specific standards have been met. As an example, one benchmark identifies dependency on supporting foundational infrastructure networks, such as electricity, natural gas, or petroleum. The series of questions determines, among other things, whether the asset requires electricity, natural gas, or petroleum to operate. If the asset does require one of these, the contractor must provide a description, and must then assess whether the benchmark for each of these networks is met.

ASD(HD&ASA) Has Been Developing a Remediation Guide

ASD(HD&ASA) has been developing the DOD Remediation Planning Guide for the DCIP remediation process in order to provide a standardized process for determining, planning, and implementing remediation actions for DOD personnel involved in remediating risks and supporting overall DOD mission assurance.[10] The planning guide encompasses: (1) DOD-owned assets that support the National Military Strategy; (2) non-DOD-owned assets that support the National Military Strategy (i.e., government-owned infrastructure, commercial-owned infrastructure, and the defense industrial base); and (3) non-DOD-owned assets that are so vital to the nation that their incapacitation, exploitation, or destruction could have a debilitating effect on the security or economic well-being of the nation or could negatively affect national prestige, morale, and confidence.

Because proper remediation lessens the negative effect of an event, it makes sense in many cases to strengthen, through a reduction of risk, those assets critical to DOD missions. When unacceptable levels of risk are identified, an asset owner should seek to remediate them in a prioritized fashion based on their overall risk to DOD. This planning guide identifies and discusses specific actions that are essential to remediation strategy development and implementation. The planning guide calls for an effective plan of action and milestones focusing on a remediation strategy to be developed as soon as feasible following the risk assessment. The planning guide provides the basic steps for an effective plan and suggested time frames: (1) confirm ownership and prioritize risk as soon as possible after completion of assessment; (2) analyze options and determine the best approach within 30 days after a risk assessment is completed; (3) develop the remediation plan as soon as practicable, but not later than 60 days after the risk assessment; (4) implement the remediation plan within 2–4 weeks following remediation plan approval; (5) keep appropriate officials informed at plan commencement and within 2–4 weeks of remediation plan completion; and (6) execute follow-up actions no more than 3 years after risk assessment.

The planning guide also includes a chapter focused on DIB remediation. It states that the remediation measures for the DIB focus on facilitating relationships and sharing information to implement the appropriate level of protection. The chapter referring to the DIB is designed to assist asset owners, operators, and DOD managers in determining whether a

[10]DOD, Defense Critical Infrastructure Program, *DOD Remediation Planning Guide*, Version 1.0 (Apr. 20, 2007).

remediation action is justified and required. The DIB sector remediation process includes a step-by-step approach for analyzing issues and making judgments. It describes a remediation process that will help preserve privately owned DIB critical asset capabilities. ASD(HD&ASA) officials told us it was designed in a general way without suggested time frames because of the voluntary nature of the DIB participation in the DCIP.

DOD Will Need to Address Several Key Challenges in Implementing Its DIB Risk Management Approach

DOD faces several key challenges in implementing its DIB risk management approach and will need to address them to ensure that its approach is sound and its progress can be measured. First, the critical asset list used by DCMA does not incorporate comprehensive, mission-essential task information from the military services. Second, the prioritization model used by DCMA has not yet undergone external technical review and lacks both contractor-specific data and comprehensive threat information. Third, DCMA is not scheduling and conducting its vulnerability assessments in accordance with the asset rankings in its prioritization model. Fourth, DOD lacks a plan for identifying and addressing challenges in assessing vulnerabilities of critical foreign contractors.

Critical Asset List Does Not Yet Have Comprehensive Mission-Essential Task Information

DCMA is not currently obtaining comprehensive information from all of the combatant commands and services needed to develop a critical asset list that is linked to DOD's mission-essential tasks. Both the 2006 DIB critical asset list and the list in development for 2007 do not reflect data from all the combatant commands and services using mission-essential task information. The DOD risk management approach calls for identifying DIB assets critical to supporting combatant commanders' mission-essential tasks that would result in DOD-wide mission failure if the asset were to be damaged, degraded, or destroyed. According to DCMA and the services, DCMA and the Army and Navy provided most of the data for the 2006 critical asset list, but the Air Force did not provide input for the list. In responding to DCMA's request for the 2007 critical asset list, the Air Force limited its participation to the review and validation of DIB critical assets identified and compiled by DCMA, which used DCMA's methodology only. This service has made no independent submission of DIB-like assets to DCMA. DCMA officials told us they were aware of the need to link DIB assets to mission-essential tasks. The DIB sector assurance plan calls for identifying assets critical to supporting combatant commanders' mission-essential tasks that would result in DOD-wide mission failure if the asset were to be damaged, degraded, or destroyed, and DCMA says it plans to continue to collaborate and strengthen

relationships with the combatant commands and other DOD organizations in identifying DIB assets and systems supporting their critical missions.

According to OSD officials, the services are still working on identifying the mission-essential tasks and the defense critical assets that support these tasks, including DIB defense critical assets. The method for identifying critical DIB assets has evolved, and refinements are continuing. Thus far, a plan with targets and time frames has not been established for identifying all of the mission-essential tasks for all of the services.

DCMA's Prioritization Model Has Not Yet Been Reviewed and Does Not Yet Have Contractor-Specific Data or Comprehensive Threat Information

The asset prioritization model has not undergone external technical review. Further, some needed contractor-specific data were missing for a number of the critical assets. Additionally, the absence of comprehensive threat data undermines the utility of the index score for prioritizing contractors.

Model Has Not Yet Had External Technical Review

Our review of the asset prioritization model revealed that weighting factors were selected and much of the input data were determined according to subjective decisions made with only limited review. According to the DCMA official who developed the model, the subjectivity involved in assigning the precise values of the weights in the model is the most controversial aspect of the model. Cross-disciplinary collaboration and peer review are, in our opinion as well as that of DOD officials with whom we spoke, important means of validating modeling strategies. As of the time of our review, DCMA had not had its model independently reviewed.

The model, created in September 2004, has undergone a number of refinements, and more are planned. According to the DCMA staff member who developed the model, he is the only individual who fully understands the model and all submodels and is responsible for assigning factor risk scores to each asset. Future initiatives for refining the model include (1) developing submodels in 2007, (2) addressing issues regarding data absence and data obsolescence in 2008, (3) developing guidance for others on how to use the model (no established target date), and (4) moving from a spreadsheet format to a Web-based application (no established target date). Without independent formal review of its asset prioritization model,

DCMA cannot be assured that the model is valid and suitable for its intended purpose.

Needed Contractor-Specific Data Are Missing

Our review of the model also revealed that contractor-specific data were missing for a number of the critical assets. DCMA collects open-source and in-house statistical data on contractor operations, but it lacks some needed contractor-specific information from the DIB contractors on their operations for use in the model. DCMA has undertaken two surveys to obtain these needed data and is planning a third survey, but these efforts depend on contractors' willingness to provide business sensitive information and they have thus far not been fully successful.

The model does not distinguish between assets marked as high risk by default for lack of data and those for whom data corroborate the high-risk designation. Our review of the asset prioritization model found that DIB contractors with similar entries based on missing data for several factors may not be differentiated one from another; it was not always apparent whether some contractors were identified as high risk because of an unavailability of data or the presence of data that justified the identification. The ability to distinguish between high scores due to risk and high scores due to missing data has important implications for resource allocation, for data collection and assessment, and for risk remediation. Additionally, prioritization of data collection should focus on those items that are most mission-critical and have the highest weight in the model's scores.

DCMA has conducted two surveys, called industrial capabilities assessments, to obtain contractor-specific information on DIB assets, but both of these efforts have met with limited response rates. DCMA officials said this was due at least partly to contractors' reluctance to provide information. In 2004 DCMA sent a questionnaire to obtain additional information from DIB contractors. DCMA had requested this information using a cover letter to the companies signed by the Assistant Secretary of Defense for Homeland Defense (ASD-HD) and coordinated with DCMA officials in the field. DCMA officials said that these steps were taken to help ensure a greater response to the survey. Nevertheless, of those responding, some of the survey forms were incomplete and some of the data provided were determined to be unreliable. In 2005, DCMA sent a revised questionnaire, but it was not administered with the same level of discipline used in the first one. For example, it did not use DOD on-site personnel to help ensure high response rates, and only 30 percent of those surveyed responded. Again, responses were incomplete and some of the data were not considered reliable. DOD officials said that contractors

were more reluctant to provide certain types of data, such as financial, disaster planning, reconstitution, and especially forecast data. DCMA did not conduct a survey in 2006.

DCMA is planning another effort in fiscal year 2007 to send out a revised capabilities-assessment questionnaire to DIB contractors. DCMA officials are in the process of revising and expanding on the assessment to be sent to contractors to more specifically address critical infrastructure protection. Once DCMA has finalized the critical asset list for 2007, it is planning to conduct a new industrial capabilities survey. However, it will take several months for DIB critical contractors to receive, fill out, and return the industrial capabilities survey; and DCMA has not identified specific steps to ensure that this survey receives a high response rate with quality information.

Model Does Not Yet Incorporate Comprehensive Threat Information

Our review of DOD's asset prioritization model also revealed a lack of comprehensive threat information. DOD officials told us that intelligence-gathering agencies currently provide information to DCMA through ad hoc agreements, as opposed to a more formalized arrangement. The collection and analysis of DIB-related intelligence information has evolved over time between such agencies as DSS, Counter Intelligence Field Activity, and DCMA. According to DCMA as well other DOD officials, DCMA does not receive comprehensive threat information from the appropriate intelligence agencies to enable it to accurately prioritize DIB assets. These intelligence agencies include the National Counterterrorism Center, DHS's Office of Intelligence and Analysis and its Homeland Infrastructure Threat and Risk Analysis Center, the FBI, and others. While DCMA obtains information for prioritization from the Counter Intelligence Field Activity, DCMA does not routinely obtain full threat information from these other intelligence agencies. The absence of comprehensive threat data undermines the utility of the index score for prioritizing contractors. Until DCMA develops and implements procedures for obtaining the threat data needed, it cannot rely on the outputs of its asset prioritization model.

Vulnerability Assessments Are Being Conducted without Benefit of Asset Prioritization Rankings

DCMA is conducting its vulnerability assessments on critical DIB assets according to contractor accessibility and without regard for those assets' respective prioritization model rankings. According to DCMA, one purpose of the prioritization model is to rank critical assets and to use this order to prioritize assessments. DCMA should schedule and conduct its vulnerability assessments on the critical DIB assets based upon their respective rankings as validated in the asset prioritization model.

Furthermore, DOD has not established targets or time frames for resolving this issue.

The assessments to be performed should be identified from a comprehensive critical asset list that has been ranked based on a reliable asset prioritization model. However, DCMA has not used the rankings from its asset prioritization model to schedule outreach visits or on-site vulnerability assessments. According to DCMA officials, a high score on the model should result in DCMA's contacting the contractor to conduct a vulnerability assessment. However, they said that coordinating on-site assessments is complicated and highly sensitive. DCMA officials say that lack of facility security clearances complicates their efforts to get DIB contractors to participate in DOD's risk management program because DCMA cannot inform uncleared contractors that they are on the classified critical asset list or discuss with them vulnerabilities found at their facilities. Consequently, officials have devoted outreach efforts, first, to those contractors at facilities having the necessary security clearances, and next, to those that DCMA officials believe would be most amenable to undergoing an assessment. About 52 percent of the DIB facilities identified as critical lack security clearances for the facility or any of its personnel, and thus cannot receive vulnerability assessments or discuss needed remediation actions. DSS officials told us that, though they recognized that many critical contractors did not have facility security clearances, DSS lacks the resources needed to preemptively clear all critical DIB facilities.

In further explaining why they have not followed the prioritization ranking in conducting assessments, DCMA officials said that because private-sector DIB contractors' participation in the program is voluntary, DCMA must rely on the contractors' willingness to cooperate and provide information. According to DCMA officials, some DIB contractors have had concerns about sharing information that they consider proprietary, and about the possibility of incurring additional costs and liabilities to correct any vulnerabilities identified as part of this program as a result of sharing this information. These concerns regarding sharing information with DOD were echoed by some of the DIB contractors with whom we spoke, for a variety of reasons. For example, when asked about his willingness to share certain information with DOD, one DIB contractor we spoke with said that he was concerned that information that he deemed proprietary or potentially damaging to the company could somehow be released or disclosed, and he was unsure how DOD would protect such information. Furthermore, DOD officials noted that some significant DIB contractors are involved in classified, special access programs that could involve military mission-essential tasks and as a result may not be allowed or

willing to share certain types of information. They also noted that there is no similar effort to identify critical DIB assets from the classified special access program perspective. Consequently, some significant critical DIB assets may not currently be included as part of the program.

DCMA officials told us that, in order to overcome resistance from those DIB contractors that may be reluctant to share information and participate in the program, they have developed tactics that in some cases have been successful in promoting greater voluntary participation. For example, in at least one case, DCMA requested that a high-level DOD official reach out to the contractor directly and make the informational request. Also, DCMA officials told us that they develop memoranda of agreement with contractors that delineate what the on-site assessment will entail, what the assessment team and the company are agreeing to do, and the manner in which the contractor's information will be used and protected. DCMA officials told us that while these steps have resulted in progress, they have also been time-consuming and have affected the sequence according to which critical DIB contractors have been scheduled for assessment.

The program, and DCMA's outreach and educational efforts in eliciting contractor information, continue to evolve. For example, the sector-specific plan states that DOD plans to develop an accreditation plan for identifying and certifying Protected Critical Infrastructure Information (PCII) under DHS's PCII program. The PCII program was established by DHS pursuant to the Critical Infrastructure Information Act of 2002.[11] The act provides that critical infrastructure information[12] that is voluntarily submitted to DHS[13] for use by DHS regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement, shall receive various protections, including exemption from disclosure under the Freedom of Information Act.[14] If such information is validated by DHS as PCII, then the information

[11]The Critical Infrastructure Information Act was enacted as Title II, Subtitle B of the Homeland Security Act of 2002. Pub. L. No. 107-296 (2002).

[12]"Critical infrastructure information" is defined at Section 212 of Pub. L. No. 107-296 (2002).

[13]DHS's final rule implementing the Critical Infrastructure Information Act identifies procedures for indirect submissions to DHS through DHS field representatives and other federal agencies.

[14]5 U.S.C. § 552.

can only be shared with authorized users.[15] Before accessing and storing PCII, organizations or entities must be accredited and have a PCII officer. Authorized users can request access to PCII on a need-to-know basis, but users outside of DHS do not have the authority to store PCII until their agency is accredited. However, the lack of accreditation does not otherwise prevent entities from sharing information directly with DOD.

However, we noted in our April 2006 report that nonfederal entities continued to be reluctant to provide their sensitive information to DHS because they were not certain that their information will be fully protected, used for future legal or regulatory action, or inadvertently released.[16] Since our April report, DHS published on September 1, 2006, its final rule implementing the act, but we have not examined whether nonfederal entities are more willing to provide sensitive information to DHS under the act at this time, or DOD's cost to apply for, receive, and maintain accreditation. However, one of the DIB contractors we interviewed mentioned generally that while some advances have been made in information protection, such as the establishment of the PCII program, the contractor continues to be concerned that the program has yet to demonstrate that it can provide good security for contractor-provided information, and remains wary about damage from public or competitor disclosure.

DCMA officials also pursued new legislation and additional provisions for the Defense Federal Acquisition Regulation in order to, in their view, potentially increase industry participation, but these changes were ultimately not enacted. For example, DCMA officials had drafted a legislative proposal that stated that "critical supplier assessments and company specific assessments developed under the Defense Critical Infrastructure Program, evaluating the security of Defense Critical Suppliers, shall not be disclosed under the Freedom of Information Act."[17]

[15]For more information on the procedures by which PCII may be shared, see DHS's *Procedures for Handling Critical Infrastructure Information*, 6 C.F.R. 29.

[16]GAO, *Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information*, GAO-06-383 (Washington, D.C.: Apr. 17, 2006).

[17]The Freedom of Information Act, codified at 5 U.S.C. 552, states that agencies shall make available certain documents for public inspection and copying. However, there are exemptions to this requirement. For example, FOIA does not apply to matters that are "trade secrets and commercial or financial information obtained from a person and privileged or confidential."

However, DCMA officials told us that the legislative proposal was ultimately not approved to be included in the DOD legislative proposals that are sent to the Congress for consideration and there are no current plans within DOD to pursue this legislation. In addition, DCMA officials also pursued the addition of clauses to the Defense Federal Acquisition Regulation. The language that was proposed would have included several provisions pertaining to the critical infrastructure of the defense industrial base, such as stating that the contractor shall be responsible for the overall organizational physical protection and security of its own critical infrastructures; have in place a comprehensive security plan relating to overall plant and facility security designed to protect its critical infrastructures; that the government shall be permitted to conduct or facilitate vulnerability and mission assurance assessments under the DCIP. However, these changes were ultimately not submitted to the Defense Acquisition Regulation Council.[18]

DCMA Does Not Yet Have a Plan for Assessing Foreign DIB Critical Assets

DCMA has not established a plan to deal with the potential challenges inherent in assessing vulnerabilities of foreign contractors. In order to do so, DCMA needs to coordinate with other agencies, such as the Department of State, to develop strategies to better ensure that foreign contractor vulnerabilities can be identified and addressed. DCMA has not conducted any assessments of foreign contractors.

The critical asset list identifies nine foreign contractors. DCMA planned to conduct a pilot assessment on one of these contractors in 2006, but did not do so, according to DCMA officials, because procedures are not yet in place for assessing foreign suppliers of products manufactured overseas. The DIB sector-specific plan recognizes the challenge involved when DIB assets are located in foreign countries, and states that where DIB assets are located in foreign countries many of the plan's proposed activities could be perceived as U.S. government intrusion into sovereign areas of the host country, particularly with respect to threats and vulnerabilities. The plan also recognizes that DOD and the DIB Sector Coordinating Council must ensure that DIB protection activities are coordinated with U.S. embassies and host governments; that where pertinent treaties exist,

[18]The Defense Acquisition Regulations Council establishes operating procedures for the Defense Acquisition Regulation System to facilitate development and processing of procurement and contracting policy, procedures, clauses, and forms, for approval by the Director of Defense Procurement.

activities should conform to them; and that a strategy needs to be developed for an action plan in foreign countries with DIB assets.

Conclusions

DOD is in the process of implementing a risk management approach to identify, prioritize, evaluate, and remediate threats, vulnerabilities, and risks to critical DIB assets, including those DIB assets that are critical to achieving DOD's mission-essential tasks. Several key challenges to the implementation of this program need to be addressed in order for DOD to be able to ensure that its approach is sound. First, in identifying and prioritizing critical DIB assets, DOD is not currently incorporating data reflecting mission-essential task information from all of the services. Second, in order for DOD's asset prioritization model to be reliable, the model would benefit from appropriate external technical review, and it also lacks selected contractor-specific data that need to be provided by DIB contractors, as well as comprehensive threat information from the appropriate intelligence agencies. Without a comprehensive list of critical assets and a reliable asset prioritization model, DOD cannot ensure that it has identified the most important DIB critical assets, as is necessary for carrying out the National Military Strategy. Third, DOD is currently scheduling and conducting assessments based on contractor amenability and security clearance status, rather than on the rankings assigned to critical DIB assets according to its asset prioritization model. Unless DOD assesses assets based on their rankings determined by a reliable asset prioritization model, DOD will not be in a sound position to know that it is assessing the most critical DIB assets or making the best use of limited resources. Fourth, DOD has not yet developed a plan for identifying and addressing potential challenges in assessing vulnerabilities of critical foreign DIB contractors. As a result, vulnerabilities in these critical foreign contractors can potentially threaten their availability to DOD. Until all of these issues are addressed, DOD will lack the visibility it needs over critical DIB asset vulnerabilities, will be unable to encourage critical DIB contractors to take needed remediation actions, and will be unable to make informed decisions regarding limited resources.

Recommendations for Executive Action

To manage the complete development of the risk management approach to better ensure its effectiveness we recommend the Secretary of Defense direct the ASD(HD&ASA) to develop a management framework that includes targets and time frames and undertakes the following steps:

- Obtain comprehensive data from all the combatant commands and services based on mission-essential task information, and incorporate

these data with those set forth in DCMA guidance, to develop a comprehensive list of the critical DIB assets.

- Improve the reliability of its asset prioritization model by
  - obtaining the appropriate external technical review;
  - developing a detailed plan for improving response rate and data quality from DIB contractors in conducting its next capabilities survey, to ensure that DCMA obtains contractor-specific data needed for establishing priorities; and
  - identifying and developing procedures for obtaining comprehensive threat information from the appropriate intelligence agencies, including DHS, the FBI, and others to use as model inputs to prioritize DIB assets and conduct vulnerability assessments.
- Schedule and conduct vulnerability assessments on the critical DIB assets based on their respective rankings as validated in the asset prioritization model, to ensure that the most critical DIB assets are assessed in a timely manner and DOD maximizes its use of limited resources.
- Prepare a plan to collaborate with the Department of State and other agencies, as appropriate, to develop options to identify and address potential challenges in assessing vulnerabilities of critical foreign contractors.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD partially concurred with all four recommendations. In its response, DOD cited actions it planned to take that are generally responsive to our recommendations. DOD also provided us with technical comments, which we incorporated in the report, as appropriate. DOD's response is reprinted in appendix II.

DOD partially concurred with our recommendation to develop a management framework that includes targets and time frames and to obtain comprehensive data from all the combatant commands and services based on mission-essential task information. DOD stated that DCMA is aware of the need to link DIB assets to mission-essential tasks and that ASD(HD&ASA) has developed a draft DOD instruction to formalize this process. DOD also said that DCMA is incorporating this framework into its process for critical asset identification and that ASD(HD&ASA) is developing a DCIP program plan that will address targets and time frames for achieving these goals. DOD commented that this plan should be completed by the first quarter of fiscal year 2008.

DOD partially concurred with our recommendation to improve the reliability of its asset prioritization model by obtaining the appropriate external technical review, needed contractor specific data, and

comprehensive threat information from the appropriate intelligence agencies and stated that DCMA had coordinated the review of the asset prioritization model with the DOD Modeling and Simulation Office, the Canadian Department of National Defense, and various DOD activities. However, at the time of our review, DCMA had not yet coordinated the review of the asset prioritization model with these offices, and other feedback on the model was informal and undocumented. We found that the model has had a number of refinements over the years and that there are fundamental processes that have not been reviewed. We believe that DOD is responsive to our recommendation in its comment that DCMA is open to further technical review of the APM and will work with ASD(HD&ASA) to identify credible and capable subject matter experts to support this effort, and we would stress the need to develop targets and time frames for completing these actions. DOD also commented that developing a detailed plan may improve the contractor response rate and data quality; but noted that participation by industry to provide information is voluntary and contractors continue to be concerned with the release of certain types of data, such as financial, disaster planning, reconstitution, and especially forecast data. We agree that contractor participation is voluntary but there are strategies available to DCMA to improve response rates. As noted in our report, DCMA response rates declined when the process lacked a coordinated plan. DOD also stated that a draft DOD Instruction 3020.nn identifies the intelligence agencies that DCMA will work with to obtain threat and hazard information on DIB critical assets. However, we found that the draft instruction only identified the Under Secretary of Defense for Intelligence to secure support from other DOD activities and does not reference securing support from agencies we note in the report such as DHS and the FBI. As noted in DCMA's May 2007 sector assurance plan, barriers in the area of threat assessment information and sharing information still require management attention.

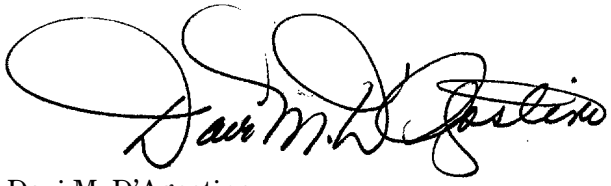
DOD partially concurred with our recommendation to schedule and conduct vulnerability assessments on the critical DIB assets based on their respective rankings as validated in the asset prioritization model, and noted a number of factors that exist that may prevent scheduling assessments in accordance with the model's numerical ranking. For example, DOD noted if a contractor on the list is reluctant at first or refuses to participate, it should move to the next contractor on the list, while simultaneously negotiating with the first contractor to gain its participation. DOD also noted that the list is dynamic and may change year-to-year. In addition, DOD may accept the vulnerability assessments performed internally by the contractor providing the company meets

established requirements and standards. We believe that the approach described by DOD acknowledges the intent of our recommendation to conduct assessments on the basis of those deemed most critical. We recognize that there will be reasons to conduct assessments out of order, and would expect that those decisions will be documented.

DOD partially concurred with our recommendation to prepare a plan to collaborate with the Department of State and other agencies, as appropriate, to develop options to identify and address potential challenges in assessing vulnerabilities in foreign critical DIB assets. DOD stated that DCMA efforts to date have focused primarily on Continental United States assets as they constitute 95 percent of the assets on the critical asset list and that the DIB sector specific plan recognizes the challenges involved when DIB assets are located in foreign countries. DOD further stated that DCMA will continue to work with ASD(HD&ASA) in laying out a framework to both address the issue and to work in collaboration with other government agencies, including the Department of State.

As agreed with your offices, we are sending copies of this report to the Chairman and Ranking Member of the Senate and House Committees on Appropriations, Senate and House Committees on Armed Services, and other interested congressional parties. We also are sending copies of this report to the Secretary of Defense; the Secretary of Homeland Security; the Director, Office of Management and Budget; and the Chairman of the Joint Chiefs of Staff. We will make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact me at (202) 512-5431 or by e-mail at dagostinod@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.



Davi M. D'Agostino
Director, Defense Capabilities and
Management

Appendix I: Scope and Methodology

To conduct our review of the Department of Defense's (DOD) defense industrial base (DIB) program, we obtained relevant documentation and interviewed officials from the following DOD organizations:[1]

- Office of the Secretary of Defense (OSD)
  - Under Secretary of Defense for Personnel and Readiness, Information Technology Division;
  - Under Secretary of Defense for Acquisition, Technology, and Logistics, Office of the Deputy Under Secretary of Defense for Industrial Policy;
  - Under Secretary of Defense for Intelligence, Counterintelligence & Security, Physical Security Programs;
    - DOD Counterintelligence Field Activity, Critical Infrastructure Protection Program Management Directorate;
  - Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD[HD&ASA]), Critical Infrastructure Protection Office;
  - Assistant Secretary of Defense for Networks and Information Integration, Information Management & Technology Directorate;
- Joint Staff, Directorate for Operations, Antiterrorism and Homeland Defense
- Defense Threat Reduction Agency (DTRA), Combat Support Assessments Division
- Military Services
  - Department of the Army, Asymmetric Warfare Office, Critical Infrastructure Risk Management Branch;
  - Department of the Navy
    - Office of the Chief Information Officer;
    - Mission Assurance Division, Naval Surface Warfare Center, Dahlgren Division, Dahlgren, Virginia;
    - Headquarters, U.S. Marine Corps, Security Division, Critical Infrastructure Protection Office;
  - Department of the Air Force, Air, Space and Information Operations, Plans, and Requirements, Homeland Defense Division;
- Headquarters, Defense Intelligence Agency, Office for Critical Infrastructure Protection & Homeland Security/Defense;
- Headquarters, Defense Information Systems Agency, Critical Infrastructure Protection Team;
- Headquarters, U.S. Strategic Command, Mission Assurance Division, Offutt Air Force Base, Nebraska

[1]DOD organizations are located in the Washington, D.C., metropolitan area unless indicated otherwise.

To examine the status of DOD's efforts to develop and implement a risk management approach, we reviewed Homeland Security Presidential Directive 7, the Homeland Security Act of 2002, and the National Infrastructure Protection Plan as they relate to the DIB sector-specific and sector assurance plans, as well as other studies conducted by GAO, the Congressional Research Service, and the DOD Inspector General concerning risk management and defense critical infrastructure. We discussed with DOD officials the requirements for a risk management plan for the DIB and the status of the approach's implementation. We also reviewed and discussed information and data on the Defense Contract Management Agency's (DCMA) efforts to identify, assess, and remediate critical DIB assets. Specifically, we evaluated the basis for the criteria DCMA established and used to identify important and critical DIB assets; the ways in which these criteria were used by each of the services to help identify important and critical DIB assets; and the ways in which foreign contractors were being identified. We evaluated information concerning the development of the asset prioritization model, the factors used to rank order the critical assets, the refinements that have been made and planned as the model matures, and the outcomes produced by applying the model to the fiscal year 2006 critical asset list. We reviewed the standardized mission assurance assessment process for critical DIB assets, the development of standards to be used, the training for teams to conduct assessments, the reports on six pilot vulnerability assessments performed in fiscal years 2006 and 2007, and lessons learned to be incorporated in future assessments. We reviewed the remediation planning guidance DOD is developing for the Defense Critical Infrastructure Program (DCIP) generally, and we compared the overall guidance to that being developed for the DIB. We also met with the National Guard Bureau and one of the state National Guard teams that conducts DIB sector vulnerability assessments.

To examine the challenges faced by DOD in developing and implementing its approach, we assessed the extent to which key steps in the planned approach have been implemented. We compared DCIP policies for identifying mission-essential tasks and related defense critical assets with DCMA's criteria for identifying a critical DIB asset; and we discussed reasons for the differences with OSD, ASD(HD&ASA), DCMA, and the services. We assessed the development and use of DCMA's asset prioritization model, including discussions with DCMA and OSD about the requirements for models used within DOD to undergo external technical review and to incorporate all the needed data in order to ensure the model's validity and suitability. We reviewed methods DCMA has used previously to obtain contractor-specific data, as well as methods planned

for future efforts, to ensure that DCMA will obtain more complete information. We discussed with DCMA and DOD intelligence agency officials the threats to the DIB and the availability of specific threat information to DCMA. We compared the assessments being conducted with the rankings of the critical DIB contractors in the asset priority model, and we discussed with DCMA officials why they have not followed the rankings and the challenges that they have encountered as they have begun working with private-sector contractors. We reviewed DCMA's efforts to encourage reluctant private-sector DIB contractors to participate in the program, including potential changes suggested for the Defense Federal Acquisition Regulation that were ultimately not enacted. We also reviewed DCMA's current efforts to work with DHS to develop an accreditation approach for identifying and certifying Protected Critical Infrastructure Information, and steps taken by DCMA to overcome resistance. We spoke with a non-probability sample of DIB contractor officials generally about their willingness to participate in the program and the reasons for their respective views, and we discussed with DOD officials and these contractor officials the availability of data concerning foreign contractors. Their comments are not generalizable to a larger population. Lastly, we determined the extent to which DCMA has identified metrics with time frames for completing development of the risk-based management process. We conducted our work between August 2006 and June 2007 in accordance with generally accepted government auditing standards.

Appendix II: Comments from the Department of Defense

ASSISTANT SECRETARY OF DEFENSE
2600 DEFENSE PENTAGON
WASHINGTON, DC 20301-2600

HOMELAND
DEFENSE

AUG 1 5 2007

Ms. Davi M. D'Agostino
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. D'Agostino:

This is the Department of Defense (DoD) response to the GAO draft report, GAO-07-1077, "DEFENSE INFRASTRUCTURE: Management Actions Needed to Ensure Effectiveness of DoD's Risk Management Approach for the Defense Industrial Base," dated July 13, 2007 (GAO Code 350881). DoD partially concurs with all four recommendations in the report. Our response is attached.

Our point of contact for this action is Mr. William Bryan, OASD(HD&ASA), (703) 602-5730 ext. 143 or william.bryan@osd.mil.

Sincerely,

Paul McHale

Enclosure:
As stated

07/009912

GAO DRAFT REPORT – DATED JULY 13, 2007
GAO CODE 350881/GAO-07-1077

"DEFENSE INFRASTRUCTURE: Management Actions Needed to Ensure Effectiveness of DoD's Risk Management Approach for the Defense Industrial Base"

DEPARTMENT OF DEFENSE RESPONSE TO THE RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs to develop a management framework that includes targets and time frames and to obtain comprehensive data from all the Combatant Commands and Services based on mission essential task information, and incorporate these data with those set forth in Defense Contract Management Agency (DCMA) guidance, to develop a comprehensive list of the critical Defense Industrial Base (DIB) assets.

DoD RESPONSE: Partially concur. Due to the large number of DIB assets, DCMA initially focused its criteria on those assets that were important because they were sole source, used obsolete or emerging technology, were long-lead time, lacked a surge production capability, or experienced significant unit cost escalation. DCMA is aware of the need to link DIB assets to mission essential tasks. The DIB Sector Assurance Plan calls for identifying assets critical to supporting combatant commanders' mission essential tasks. The method for identifying critical DIB assets has evolved and refinements are continuing. Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (OASD (HD&ASA)) has been working with the Joint Staff, Combatant Commands, and the Services to identify their mission essential tasks and link them to critical assets. OASD (HD&ASA) has developed a draft DoD Instruction 3020.nn, "Defense Critical Infrastructure Program (DCIP) Management," which is currently out for formal staffing. This Instruction formalizes the DCIP process and procedures, outlined in the Criticality Process Guidance Document, for the identification of defense critical assets and linking them to Combatant Command and Service mission essential tasks. DCMA is incorporating this framework into their process for critical asset identification. OASD (HD&ASA) is developing a DCIP Program Plan which will address targets and timeframes for achieving these goals. This plan should be completed by first quarter FY 2008.

RECOMMENDATION 2: The GAO recommended that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs to improve the reliability of its asset prioritization model by:

- obtaining the appropriate technical review;
- developing a detailed plan for improving response rate and data quality from DIB contractors in conducting its next capabilities survey, to ensure that DCMA obtains contractor-specific data needed for establishing priorities; and

- identifying and developing procedures for obtaining comprehensive threat information from the appropriate intelligence agencies, including the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI),

and others to use as model inputs to prioritize DIB assets and conduct vulnerability assessments.

DoD RESPONSE: Partially concur. The Defense Contract Management Agency (DCMA) coordinated the review of the Asset Prioritization Model (APM) with the DoD Modeling and Simulation Office (MSO), the Canadian Department of National Defense (DND), and various DoD Activities such as the Army Industrial Base Activities. The APM was also addressed in the DIB Sector Specific Plan (SSP) and coordinated with the interagency through the Homeland Security Council. Comments received from these outside organizations were favorable to the overall structure and approach of the model. DCMA is open to further technical review of the APM and will work with OASD (HD&ASA) to identify credible and capable subject matter experts to support this effort.

Developing a detailed plan may improve the contractor response rate and data quality; however participation by industry to provide information is voluntary. As the GAO stated in their report, contractors continue to be concerned with the release of certain types of data, such as financial, disaster planning, reconstitution, and especially forecast data. DCMA has made progress and continues to work on internal processes to support the collection of information on a routine basis and improve the quality of data and the response rates through collaboration with DCMA and industry.

The draft DoD Instruction 3020.nn, "Defense Critical Infrastructure Program (DCIP) Management," identifies the intelligence agencies that DCMA will work with to obtain threat and hazard information on DIB critical assets. Additionally, an Office of the Under Secretary of Defense for Intelligence (OUSD (I)) draft DoD Instruction 5240.hh, "Counterintelligence Support to DCIP," discusses an in-depth structure and process for provision of counterintelligence support.

RECOMMENDATION 3: The GAO recommended that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs to schedule and conduct vulnerability assessments on the critical DIB assets based on their respective rankings as validated in the asset prioritization model, to ensure that the most critical DIB assets are assessed in a timely manner and DoD maximizes its use of limited resources.

DoD RESPONSE: Partially concur. The assessment process typically involves using the critical asset list, as ranked by the Asset Prioritization Model (APM), to select the Defense Industrial Base (DIB) contractor candidate for an assessment. However, there are many reasons why the numeric sequence of the model will not be rigidly followed in practice. In an effort to better utilize limited resources, the Defense Contract Management Agency (DCMA) and the National Guard may elect to perform assessments for one or more contractors in the same geographic area. Additionally, this is a voluntary program and the

contractors are under no obligation to comply with the request to have vulnerability assessments conducted at their sites. The contractors have to agree to have an assessment; and the assessment schedule cannot interfere with company production schedules. If a contractor on the list is reluctant at first or refuses to participate, the Department should move to the next contractor on the list, while simultaneously negotiating with the first contractor to gain their participation. Although time-consuming, this approach has proven to be effective. The list is dynamic and may change year-to-year. Finally, in some cases, the Department may accept the vulnerability assessments performed internally by the contractor providing the company meets established requirements and standards.

RECOMMENDATION 4: The GAO recommended that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs to prepare a plan to collaborate with Department of State and other agencies, as appropriate, to develop options to identify and address potential challenges in assessing vulnerabilities in foreign critical DIB assets.

DoD RESPONSE: Partially concur. The Defense Industrial Base (DIB) Sector Specific Plan (SSP) recognizes the challenges involved when DIB assets are located in foreign countries. The plan also recognizes that DoD and the Sector Coordinating Council must ensure that DIB protection activities are coordinated with U.S. embassies and host nation governments; that where pertinent treaties exist, activities should conform to them; and that a strategy needs to be developed for an action plan in foreign countries with DIB assets. Industry is also working closely with the Defense Contract Management Agency (DCMA) to identify foreign suppliers of key components. To date, DCMA efforts have focused primarily on Continental United States (CONUS) assets as they constitute 95% of the assets on the list. DCMA will continue to work with the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (OASD (HD&ASA)) in laying out a framework to both address the issues and to work in collaboration with other government agencies. The State Department is an active participant in the DIB Government Coordinating Council and is prepared to provide assistance.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Davi M. D'Agostino, (202) 512-5431 or dagostinod@gao.gov

Acknowledgments

In addition to the contact named above, Harold Reich, Assistant Director; Aisha Cabrer; Colin Chambers; Lionel Cooper; Kate Lenane; Anna Maria Ortiz; Terry Richardson; Matthew Sakrekoff; and Cheryl Weissman also made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548